

REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-9, 12-15, 17, 21-25, 28, and 31 are currently pending in this application. Claims 1 and 21 are independent. The remaining claims depend, directly or indirectly, from claims 1 and 21.

Claim Objections

Claims 14 and 15 are objected to for incorrect dependencies. Claims 14 and 15 have been amended to depend from independent claim 1 according to the Examiner's suggestions. Thus, withdrawal of this objection is respectfully requested.

Claim Amendments

The claims have been amended to further define the position of the portable security module with respect to the first decoder. The amended claims recite that the portable security module is "operatively connected to the first decoder on a receiving side of the digital television system." Applicant asserts that no new matter is added by way of these amendments. Support for these amendments may be found, for example, on pages 6, 8, and 10 of the Specification.

Rejections under 35 U.S.C. § 102

Claims 1-5, 21, and 22 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,870,474 ("Wasilewski"). The rejection on page 3 of the Office Action mailed December 6, 2005, lists only claims 1-5, 21, and 22 as being rejected under 35 U.S.C. § 102(b).

Applicant believes that, in view of the above amendments, all claims are now in condition for allowance. Thus, this response simply addresses dependent claims 6, 7, 12-15, and 17, together with the independent claims, as these claims are patentable for at least the same reasons as those presented. Accordingly, for the following reasons, this rejection is respectfully traversed.

The amended independent claims are directed toward a system and method for communication of data between a first decoder and a portable security module, where both the portable security module and the first decoder reside on the *receiving side* of the digital television system. That is, both the portable security module and the first decoder are located on the receiving side of a broadcast system, where the portable security module and the first decoder are used to decode/decrypt *already received* encrypted digital data. In the present invention, the portable security module can be attached to the first decoder to decrypt encrypted data received from, for example, a broadcast satellite (see Specification, page 21, line 12 and Figure 3). Thus, the portable security module is operatively connected to the decoder to communicate back and forth with the decoder *on the same side* of the digital television system, and more specifically, on the receiving side of the digital television system.

Turning to the rejection of the claims, for anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. The Application respectfully asserts that Wasilewski fails to disclose or suggest all of the limitations of the amended independent claims of the present invention.

Specifically, Wasilewski fails to disclose or suggest a portable security module operatively connected to a first decoder, where both the portable security module and the first decoder reside on the *receiving side* of the digital television system. The Examiner equates the

first decoder recited in the independent claims of the present invention to the STU (90) disclosed in Wasilewski (*see* Office Action mailed December 6, 2005, page 3 and the continuation page attached to the Advisory Action mailed March 7, 2006). Also, the Examiner equates the portable security module of the present invention to the conditional access card (24) disclosed in Wasilewski (*see* Office Action mailed December 6, 2005, page 3 and the continuation page attached to the Advisory Action mailed March 7, 2006).

In contrast to the amended independent claims of the present application, Wasilewski discloses that the conditional access card (24) resides on the transmission side, while the STU (90) resides on the receiver side of the transmission of encrypted data (*see* Wasilewski, Figure 2D and col. 19, ll. 37 – 67). Thus, it is not possible for the conditional access card disclosed in Wasilewski to be used with the STU as the portable security module is used with the first decoder in the present invention because the conditional access card and the STU reside on opposite sides of the transmission of encrypted data. In fact, the STU (90) of Wasilewski includes an integrated secure processor used for decryption purposes (*see* Wasilewski, Figure 11, col. 23, ll. 1-12). Thus, it does not make sense for the conditional access card disclosed in Wasilewski to be operatively connected to the STU (90).

In view of the above, it is clear that Wasilewski fails to disclose or suggest each and every limitation recited in amended independent claims 1 and 21. Thus, independent claims 1 and 21 are patentable over Wasilewski. Dependent claims 2-7, 12-15, 17, and 22 are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 8 and 24 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of the book “Applied Cryptography” by Schneier (“Schneier”). To the extent that this rejection may still apply to the amended claims, this rejection is respectfully traversed.

As described above, Wasilewski fails to disclose the limitations of independent claims 1 and 21. Further, Schneier fails to supply that which Wasilewski lacks, as evidenced by the fact that the Examiner relies on Schneier solely for the purpose of disclosing a symmetric cryptographic algorithm and an associated symmetric key (*see* Office Action mailed December 6, 2005, page 6). Thus, it is clear that independent claims 1 and 21 are patentable over Wasilewski and Schneier, whether considered separately or in combination. Dependent claims 8 and 24 are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 9 and 25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of the book “Applied Cryptography” by Schneier (“Schneier”). To the extent that this rejection may still apply to the amended claims, this rejection is respectfully traversed.

As described above, Wasilewski fails to disclose the limitations of independent claims 1 and 21. Further, Schneier fails to supply that which Wasilewski lacks, as evidenced by the fact that the Examiner relies on Schneier solely for the purpose of disclosing an encryption algorithm used with a session key to encrypt and decrypt data communicated between the first decoder and the portable security module corresponds to a symmetric algorithm (*see* Office Action mailed

December 6, 2005, page 7). Thus, it is clear that independent claims 1 and 21 are patentable over Wasilewski and Schneier, whether considered separately or in combination. Dependent claims 9 and 25 are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claim 23 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of U.S. Patent No. 5,835,726 ("Shwed"). To the extent that this rejection may still apply to the amended claims, this rejection is respectfully traversed.

As described above, Wasilewski fails to disclose the limitations of independent claim 21. Further, Shwed fails to supply that which Wasilewski lacks, as evidenced by the fact that the Examiner relies on Shwed solely for the purpose of disclosing that the encrypted version of the session key includes a signature value readable by the portable security module to verify the authenticity of the encrypted session key (*see* Office Action mailed December 6, 2005, page 7). Thus, it is clear that independent claim 21 is patentable over Wasilewski and Shwed, whether considered separately or in combination. Dependent claim 23 is patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 28 and 31

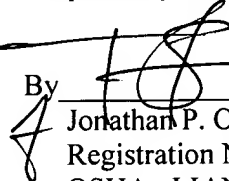
Applicant notes that the Examiner has not addressed claims 28 and 31 in any way in the Office Action mailed December 6, 2005. However, because these claims depend from independent claim 21, addressed above as being patentable over all prior art of record, Applicant respectfully submits that claims 28 and 31 contain allowable subject matter for at least the same reasons as presented above.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 11345/034001).

Dated: April 6, 2006

Respectfully submitted,

By  #45,079
Jonathan P. Osha THOMAS SCHERER
Registration No.: 33,986
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant